IN THE CLAIMS

1. (Currently Amended) A method of recognizing a fingerprint comprising:

detecting the fingerprint;

digitizing the fingerprint;

~~subtracting a digitized background from the fingerprint, resulting in a difference print;~~

sending the digitized fingerprint to a computer system to perform a match to identify~~ing~~ an individual associated with the ~~difference~~ fingerprint;

receiving extracted features from the computer system; and

confirming the match on the sensor, if the computer system indicated a match.

Claims 2-3 Cancelled.

4. (New) The method of claim 1, wherein a computing intensive match of the individual is performed on the computer system, and the sensor performs a validation requiring little computing power.

5. (New) The method of claim 1, further comprising:

receiving a final decision on the match from the sensor, such that the fingerprint isn't validated until the sensor's final decision is received.

6. (New) The method of claim 1, wherein the confirming the match on the sensor occurs on a secure processor within the sensor.

7. (New) The method of claim 1, further comprising:

updating a template in a database if the sensor confirmed the match.

8. (New) The method of claim 1, further comprising:

returning a signed template for final verification to the computer system.

9. (New) The method of claim 1, further comprising:

wherein the sensor confirms intermediate data, and the final verification is performed on the computer system.

10. (New) A biometric sensor coupled to a computer system, the biometric sensor comprising:

a sensing unit to detect a biometric;

a connection to securely transmit the biometric to the computer system for authentication and to receive a preliminary match from the computer system; and

a decision making unit to perform verification of the preliminary match and make a final decision on whether the biometric is authenticated.

11. (New) The biometric sensor of claim 10, wherein a computing intensive match of the individual is performed on the computer system, and the sensor performs a validation requiring little computing power.

12. (New) The biometric sensor of claim 10, wherein the decision making unit comprises a secure processor within the sensor.

13. (New) The biometric sensor of claim 10, further comprising:

the decision making unit to send a notification to the computer system to update the biometric template when the verification was successful.

14. (New) The biometric sensor of claim 13, wherein the updating of the biometric template comprises replacing the biometric template currently stored on the computer system with the new biometric template.

15. (New) The biometric sensor of claim 13, wherein the updating of the fingerprint template comprises adding additional information to an existing template.

16. (New) A method of using a biometric in a computer system comprising:

receiving a registration biometric data from a user;

associating the registration biometric data with an identity information;

associating access to a file or program with the identity information, such that the file or program may be auto-launched using the biometric data.

17. (New) The method of claim 16, wherein associating access comprises altering a boot sector of the file or program to require the fingerprint in order to load the file or program.

18. (New) The method of claim 16, wherein associating access comprises:

requesting a password for the file or program; and

associating the password with the identity information;

when the file or program is launched, releasing the password on biometric validation.

19. (New) The method of claim 18, further comprising:

automatically inserting the password into a password dialog, and submitting the inserted password, such that the user need not perform any action beyond making the biometric available.

20. (New) The method of claim 14, wherein associating access comprises alerting an operating system boot sector such that the system log-in is replaced by biometric validation.

21. (New) The method of claim 18, wherein the system log-in uses a user ID, but replaces the password with biometric validation.

22. (New) The method of claim 18, wherein the system log-in replaces a user ID and password combination with a single biometric validation.